# Operational Virtualized Environments

Joseph R Mountain Jr

Principal Systems Engineer

Gnostech Inc

| | |
|---|---|
| **Report Documentation Page** | *Form Approved*<br>*OMB No. 0704-0188* |

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

| | | |
|---|---|---|
| 1. REPORT DATE<br>**MAY 2011** | 2. REPORT TYPE | 3. DATES COVERED<br>**00-00-2011 to 00-00-2011** |

| | |
|---|---|
| 4. TITLE AND SUBTITLE<br>**Operational Virtualized Environments** | 5a. CONTRACT NUMBER |
| | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
| | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)<br>**Gnostech Inc,650 Louis Drive Suite 190,Warminster,PA,18974** | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S) |
| | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT

**Approved for public release; distribution unlimited**

13. SUPPLEMENTARY NOTES

**Presented at the 23rd Systems and Software Technology Conference (SSTC), 16-19 May 2011, Salt Lake City, UT. Sponsored in part by the USAF. U.S. Government or Federal Rights License**

14. ABSTRACT

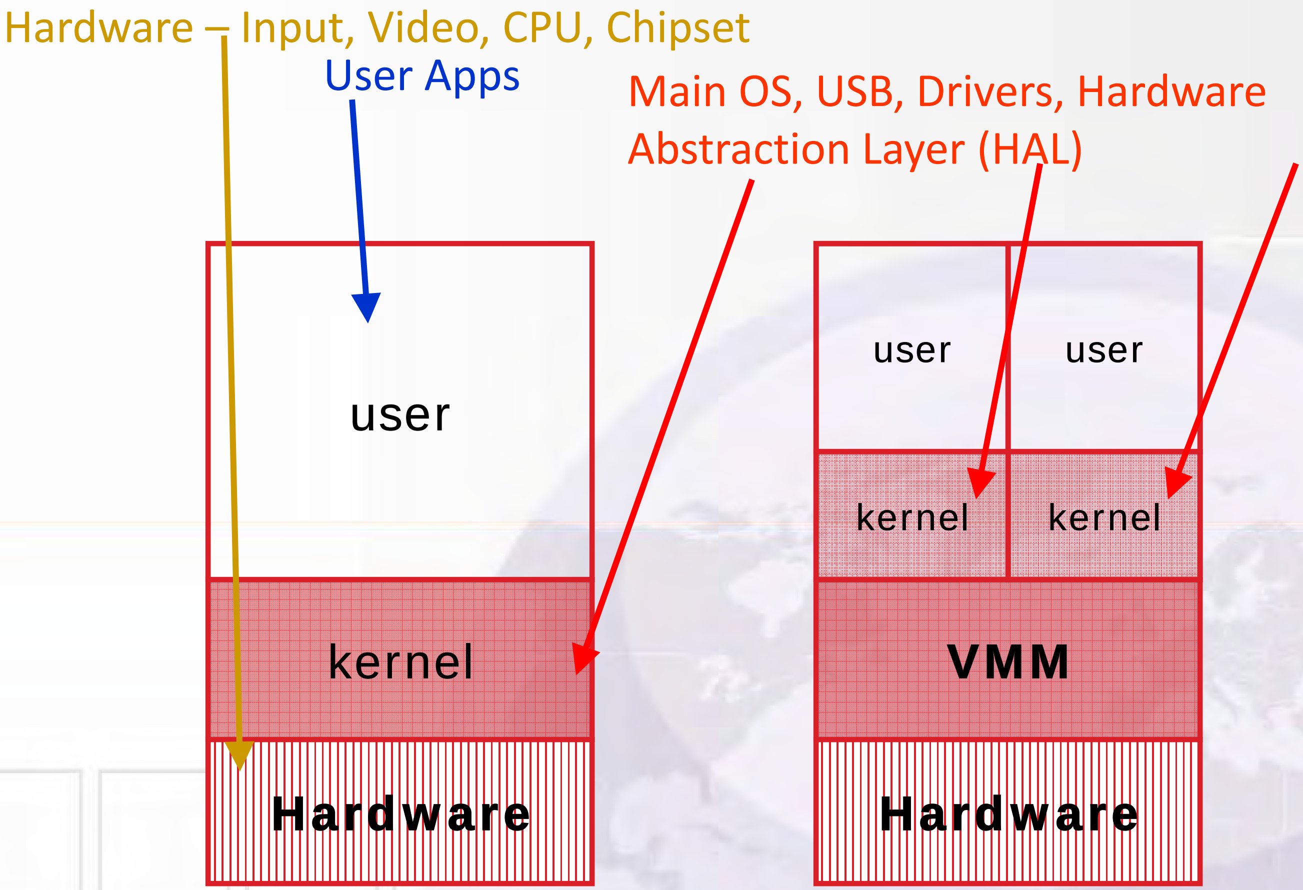
15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT<br>**unclassified** | b. ABSTRACT<br>**unclassified** | c. THIS PAGE<br>**unclassified** | **Same as Report (SAR)** | **29** | |

# Technology Obsolescence

- Hardware
  - Required External Devices are no longer supported by new computer hardware
    - PC Card such as the TUFFCard II used by the AMU in aircraft platforms to load mission data into the mission computer
      - Issues: Desktop/Laptops no longer support PCMCIA
    - SCSI-based Data Loaders
- Software
  - Windows XP End-Of-Life (EOL) – April 2014
    - No software patches produced by Microsoft after this date
    - Becomes an unsupportable product by US Government Guidelines
  - Mission Planning Environments (MPE) that support dataloaders come in a variety of OS with different security implementations
    - Includes varying security classifications

# Virtualizing the OS



Hardware – Input, Video, CPU, Chipset

User Apps

Main OS, USB, Drivers, Hardware Abstraction Layer (HAL)

user

kernel

**Hardware**

user

user

kernel

kernel

**VMM**

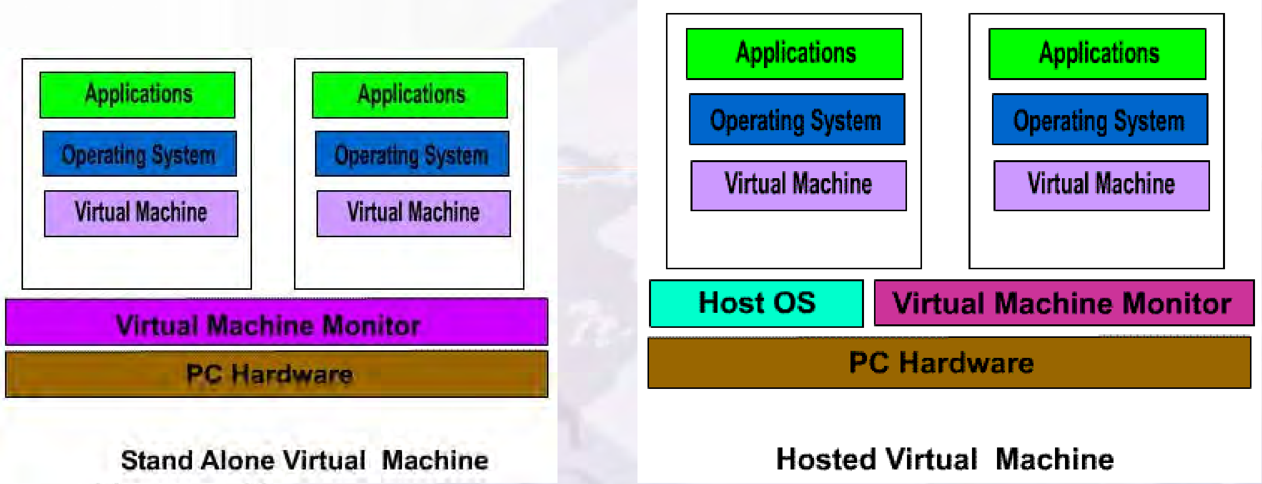
**Hardware**

Normal OS (Windows, Linux)

Virtual Machine Monitor (VMWare, Virtual PC)

# Hardware Virtual Machine Software

- Bare hardware (**Type 1** or **native** VM or Standalone VM)
- On top of an operating system (**Type 2** or **hosted** VM)

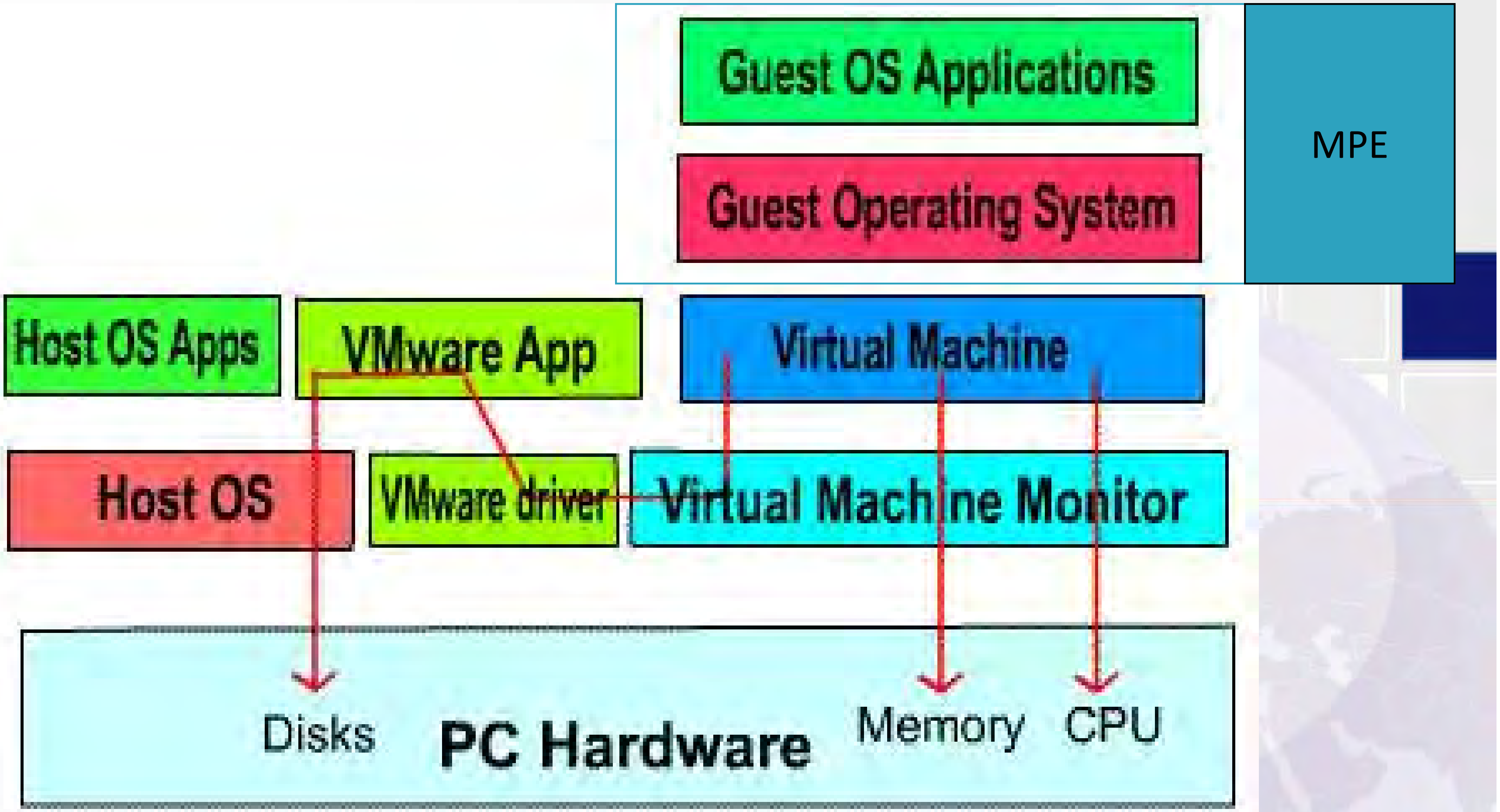


Stand Alone Virtual Machine

Hosted Virtual Machine

Virtualized Operating Environments focused on Hosted VMs

# VMWare Architecture



VMware Workstation Architecture

*knowledge* *technology* *success*

# Virtual Machine

- – Allows Multiple Operating Systems to be installed on top of Host OS (Guest OS)
- – Provides security in system and end networks
  - For example Low would have network connectivity, High would not.
- – Simultaneous access to multiple VMs
  - One or More VM can share a network connection
  - Each VM can operate at varying classification levels
  - Periods Processing
- – Full application compatibility
  - Existing Windows Applications run without modification
    - – Allows Older version of Windows to run under a VM

# So how does Virtualization fight Technology Obsolescence?

- Software
  - – Legacy Application can run under modern computer architectures
- Hardware
  - – USB provides a number of devices that can support older interfaces
    - USB to PC Card Reader is support by Virtual Machines
  - – Pass-thru Support
    - SCSI Pass-Thru Support
      - – SCSI devices are seen in the Virtual Machine

# Mission Planning Support for VM

- Support for Standalone or networked mission planning Clients
- Support for Legacy Data Loaders/External Devices
- Guest OS already defined
  - Mission Planning Environment
  - Install would need to include Appropriate VMware Drivers

# Proposed Virtualized Environment

- Virtual Machine Technology can be viewed as another COTS hardware platform
- Application is deployed and certified as a Mission Planning Environment
- Need to support Current and Legacy MPEs on one machine
  - Mission Planning on a VM plus underlying security mechanism that provide VM separation as well as Information Assurance compliance
  - MPE does not touch Host OS only Virtual Machine
    - Support for multiple VM possible by VMware Workstation

# Design of a Secure Virtualized Environment

- Elements
  - External Interfaces are defined: USB, SCSI, CD/DVD
  - Guest OS is defined: Platform Mission Platform Environment
  - Host OS Requirements:
    - No increase of admin burden
    - Transparent to user operation
    - Secure VMM

# Host OS Selection

- “Roll our own”
  - – DISA STIG Compliant Linux OS
    - Locked down
  - – VMWare Workstation for Linux
    - SELinux used to separate out one VM from another.
  - – Drivers to support Required External Interfaces
- Utilize an off the shelf Secure VMM Product
  - – NSA NetTop

# Rolling your own Secure VMM

- Resource Sharing between virtual machines
  - If two virtual machines have access to a USB Connected Device, information can flow from one VM to the other.
- Network and File Sharing
  - Two virtual machines at different security levels could communicate information across the network even internally.
- Virtual Disks
  - Virtual disk is a single file that is created in the host OS and used to encapsulate an entire guest disk, including an operating system and its applications.
    - Access to this file in the host OS could copy all information in the virtual disk to external media.
    - Restricting access to the virtual file can be remedied but a secure host OS is required.
- Program Utilities
  - Ability to cut and paste between virtual machines using a feature similar to the Windows Clipboard is a security problem for varying levels of security classification
- Host Operating System
  - Flaws in host OS design and implementation will render the virtual machine monitor and all virtual machines vulnerable

*John Scott Robin (USAF), Cynthia E. Irvine (Naval Postgraduate School), Analysis of the Intel Pentium's Ability to Support Secure Virtual Machine Monitor, Proceedings of the 9th USENIX Security Symposium, August 2000.*

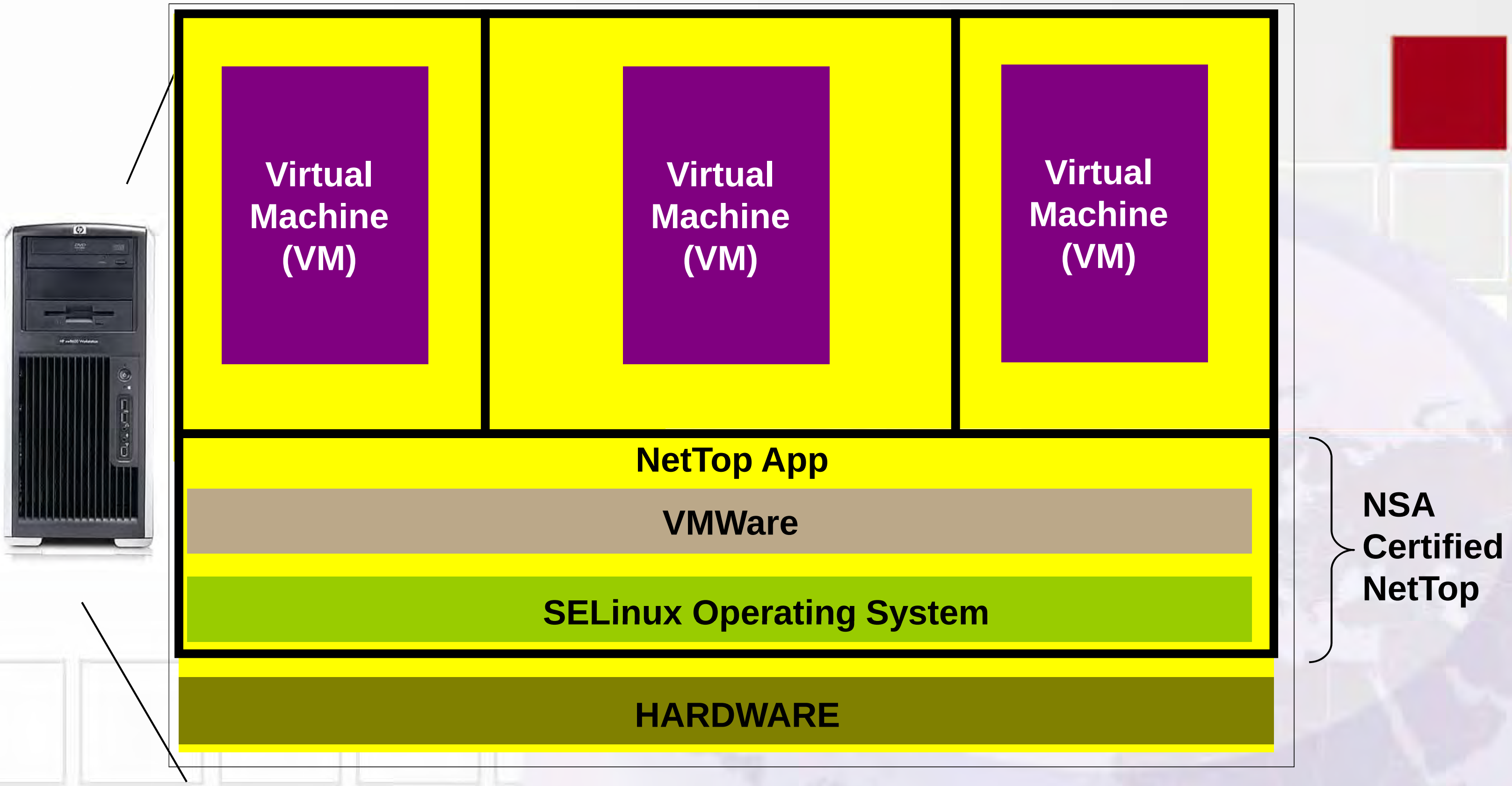
# Commercial Secure VMM

- NSA implemented VMM technology as part of its NetTop architecture
  - Original Design
    - Red Hat Linux 6.2 as Host OS
    - Unmodified end-user Windows NT OS encapsulated in a Virtual Machine
      - NSA used VMware 3.02
  - HP NetTop is a licensed commercial implementation
    - Updated to current Linux Kernel (CentOS)/VMware

# HP NetTop

- Design Notes
  - Only a single domain can simultaneously have access to a removable device (CD-ROM, USB, Floppy)
  - BIOS passwords and BIOS boot-up access must be enabled on the physical machine
  - Separate Physical Network Interface Cards are required for each Guest OS at each security level .
  - Host OS has no IP Address assigned
  - Cutting and Pasting between guests shall not be allowed

# HP NetTop


Virtual Machine (VM)
Virtual Machine (VM)
Virtual Machine (VM)
NetTop App
VMWare
SELinux Operating System
HARDWARE
NSA Certified NetTop

15

# Development of Products Built on Secure Virtualization

- Single-Level Mission Planning Multi-VM Workstation
  - Multi-VM Workstation will provide the capability to load multiple MPEs on a single host computer in order to save Size, Weight and Power (SWAP), paramount for afloat, ashore and austere environments.
- Compartment Periods Processing Multi-Level Multi-VM Workstation
  - Additional Benefits can also be derived from operating in a Multi-VM Workstation including the ability to operate at varying classification levels.

Single Level Security Use Case

# SINGLE-LEVEL MISSION PLANNING MULTI-VM WORKSTATION

# Multi-VM Mission Planning

- Elements of NSA NetTop Architecture used to support mission planning environment
  - Workstation setup with multiple instances of VMware Product
  - Host scaled back by removing unnecessary components and services.
  - Host network capability disabled
  - All networking will be provided by the mission Planning environment running at each level.

# Multi-VM Mission Planning

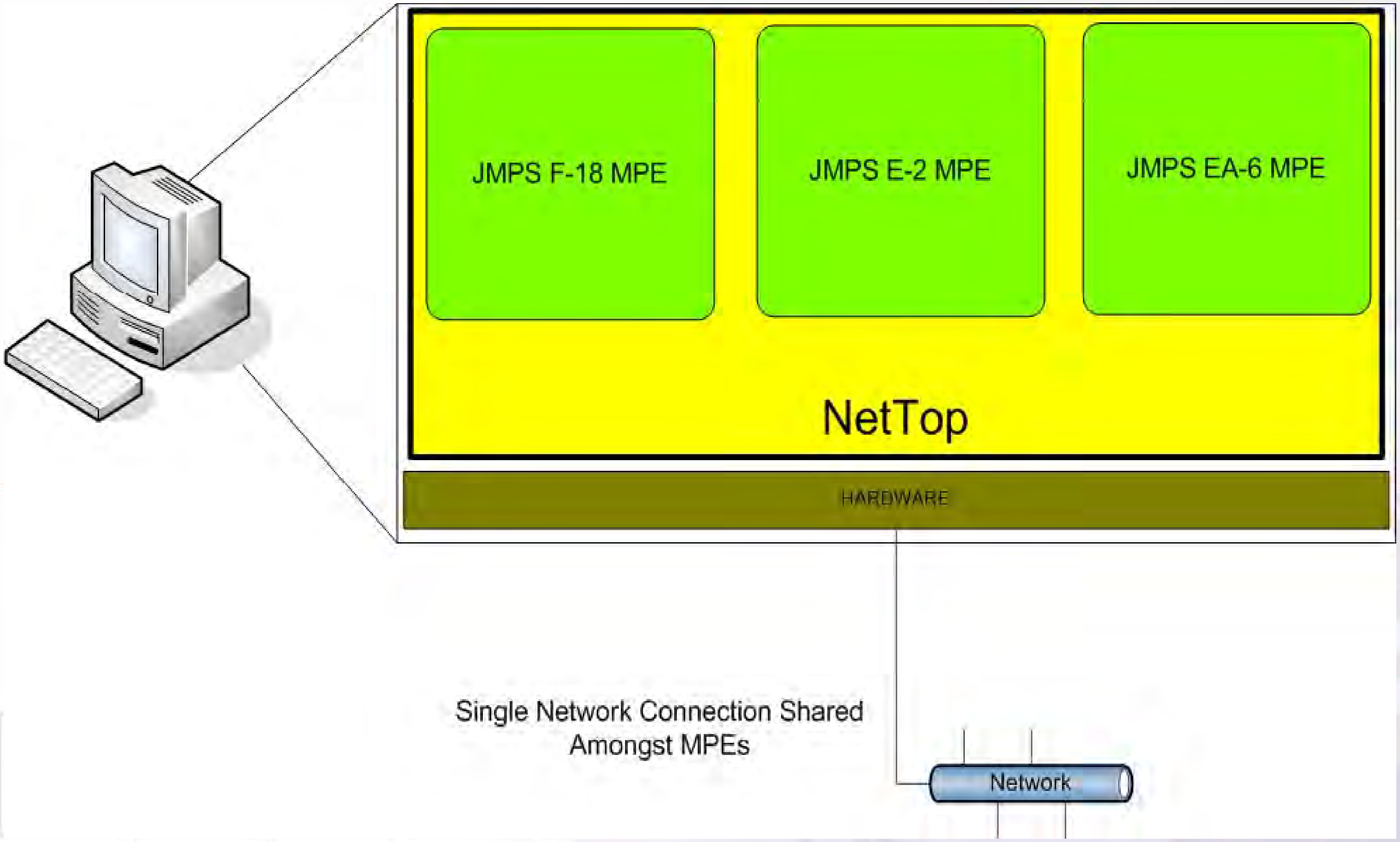
- Multiple Virtual Machine Workstation provides multiple MPEs
- System grants users the ability to simultaneously operate three separate MPEs on a single workstation
- Greatly reduces the number of workstations required by personnel to plan missions
- Prevents the need to reload MPEs when a different MPE is desired
- All MPEs have Network access

– User Accounts created on the Guest OS Network

  - Stored as part of the user accounts database on the shipboard LAN

- Optimization of System Resources to support Dataloading

# Multi-VM = Multiple MPE’s



20

# Challenges

- Limited Support for Dataloading and Poor Performance of Virtual Environments might be limiting factors
  - Dataloading
    - PC Card-based
    - SCSI-Based Data Loaders
    - USB-Based Data Loaders
    - Ethernet-based Data Loaders
  - Performance
    - High-End Workstations
      - Desktops for SCSI Support
      - Laptops for USB

Multi-Level Security Use Case

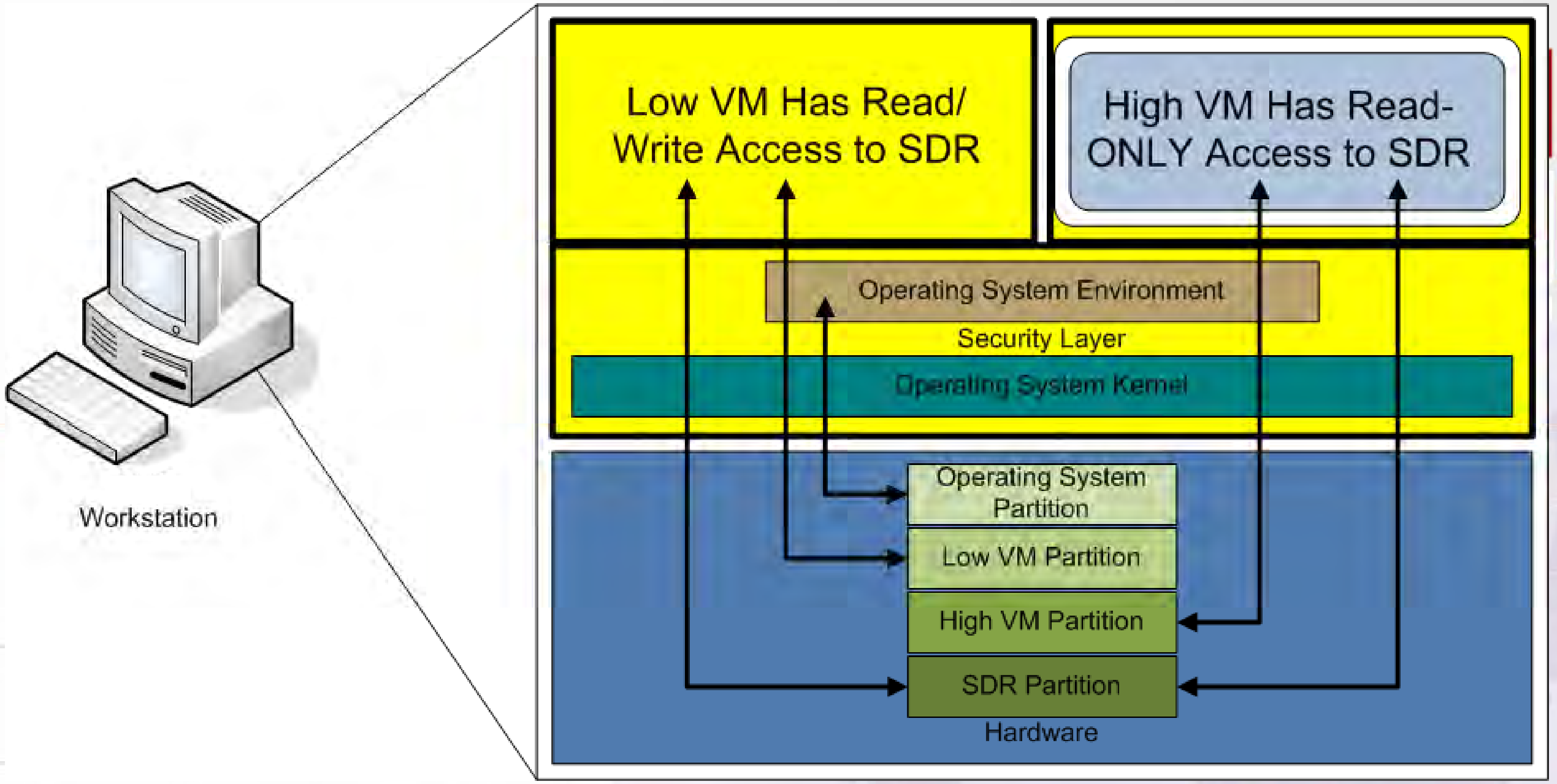
# COMPARTMENT PERIODS PROCESSING MULTI-LEVEL MULTI-VM WORKSTATION

# Multi-Level Multi-VM

- Separate Out each VM onto its own level
  - One VM designated Low, the Other High
    - Each VM has its own Network Interface Card
    - Each  VM Protected Storage Space on the Hard Disk Drive
      - Utilize Full Disk Encryption (FDE) with the capability to apply a separate encryption key for each partitions.
      - Compartmentalized Partition Encryption

# Compartmental Partition Encryption

- Hard disk partition into 4 separate encryption containers
  - Host OS Partition
  - Low Guest OS Partition
  - High Guest OS Partition
  - Shared Data Partition
- Utilize Hardware-Based Disk Encryption Methods


Low VM Has Read/ Write Access to SDR
High VM Has Read-ONLY Access to SDR
Operating System Environment
Security Layer
Operating System Kernel
Operating System Partition
Low VM Partition
High VM Partition
SDR Partition
Hardware
Workstation

# Capabilities

- Enables users to access data at **different classification levels** on a single workstation
- Enables users to load **multiple MPEs (2)** on single workstation
- Enables users to **transfer data** between different security classification levels (Low->High Only)
- System operates in "Compartmented" Periods Processing (Only one VM is active at any one time.)
  - similar to using KVM with multiple computers, Think Software KVM
  - Encrypted Partition Restricts which VM user has access to
- **Basically enables users to combine multiple workstations into a single workstation, foot print reduction.**

# Certification

- NSA NetTop Software Baseline 1.8.50 is a licensed solution
- HP NetTop Certified & Accredited by **NSA IAD Secret/Releasable–Top Secret /SCI levels**
- HP NetTop successfully completed SABI CT&E **Unclassified -Secret**
- **Meets DCID 6/3 PL4 requirements**
- UCDMO Baseline – 2.2.1

# References

- NIST SP 800-125
  - Guide to Security for Full Virtualization Technologies
- Acronyms

| | |
|---|---|
| – OS | Operating System |
| – MPE | Mission Planning Environment |
| – STIG | Security Technical Implementation Guide |
| – VM | Virtual Machine |
| – VMM | Virtual Machine Monitor |

# Contacts

- Gnostech
  - Joseph R Mountain
    - Principal Systems Engineer
    - Joseph.mountain@gnostech.com
- HP NetTop
  - Rick Supplee
    - Security Engineer for HP Secure Business
    - Rick.supplee@hp.com
  - Christianna Wolf
    - Federal Account Manager (Navy and USMC)
    - Christianna.wolf@hp.com